DHCP and DNS

CY3520

Summer 2014

DHCP Background

- Pre-DHCP, devices needed to be given an address by hand
- BOOTP (Bootstrap protocol) was invented to ameliorate this administrative headache
  - Later, this was obsoleted by DHCP
  - Can still see remnants of BOOTP when looking closer at DHCP
    - E.g., in Wireshark filtering

DHCP Background, Cont.

- Which layer does DHCP run at?
- What transport layer protocol does it employ?
- It uses a client/server architecture
  - What does this mean?
- Server has a basic responsibility to provide
  - Which items of information?
  - What types of options are also supported?

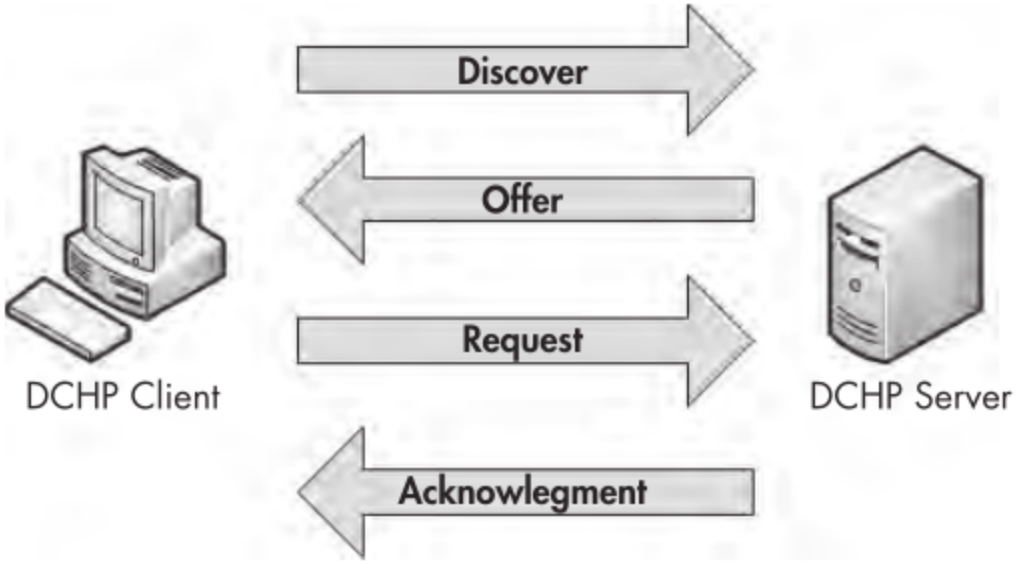
DHCP In Action

- Best way to review this protocol is to observe what it looks like on the wire

Dynamic Host Configuration Protocol				
Bit Offset	0–15		16–31	
0	OpCode	Hardware Type	Hardware Length	Hops
32	Transaction ID			
64	Seconds Elapsed		Flags	
96	Client IP Address			
128	Your IP Address			
160	Server IP Address			
196	Gateway IP Address			
228+	Client Hardware Address (16 bytes)			
	Server Host Name (64 bytes)			
	Boot File (128 bytes)			
	Options			

DHCP: DORA

- What’s the purpose of leases?



DHCP: Discover

- What are the values of the 2-tuple (IP address, port) for the client?
  - For the server? Are there any security issues with this?
  - What type of threat is this?
  - Is there any method for authentication?
    - Hint: How about RFC 3118?

DHCP: Offer

- Server addresses the offer of a particular address to a potential IP
  - Layer 2 physical address used to ensure this communication gets to the client
  - If ARP is not successful, the broadcast layer 2 address is used
- Transaction ID field in DHCP header also used to map discover to offer

DHCP: Request and Accept

- Request packet similar to discover
  - Comes from the same source address
  - Goes to the same destination address
  - Slight but significant differences in the DHCP header
- Accept packet is acknowledgement of the request
  - This pair of packets has a new transaction ID
  - Final step in the DHCP process

Releasing Process

- DORA process occurs in two situations:
  - When no IP address has been assigned
  - When the current *lease* has expired
    - Where is the lease time determined?
    - What considerations go into the lease time chosen?
- *In-lease* renewal is a truncated DORA
  - What parts of the protocol are now unnecessary?

DHCP Options

- Limited number of message types

Type Number	Message Type	Description
1	Discover	Used by the client to locate available DHCP servers
2	Offer	Sent by the server to the client in response to a discover packet
3	Request	Sent by the client to request the offered parameters from the server
4	Decline	Sent by the client to the server to indicate invalid parameters within a packet
5	ACK	Sent by the server to the client with the configuration parameters requested
6	NAK	Sent by the client to the server to refuse a request for configuration parameters
7	Release	Sent by the client to the server to cancel a lease by releasing its configuration parameters
8	Inform	Sent by the client to the server to ask for configuration parameters when the client already has an IP address

- Quite a simple protocol but much additional information can be included in the options

DHCP Server Configuration

- Quite a simplistic server to set up and configure (relatively)
  - Not a ton of features available
  - Comes with some of its own jargon
- Scopes
- Reservations
- Leases
- Allow for network booting using TFTP

DHCP Server Filtering Configuration

- Only generate responses to known clients
  - What ways could a DHCP server “know” a client?
    - What pieces of information identify a client without an IP address?
- Provides a limited filtering capability
  - What would be useful for logging purposes?
  - What is the integrity/trustworthiness of those logs?

Rogue DHCP Servers

- How could you look for the presence of rogue DHCP servers on a network?
  - What could you do to coax out their presence?
    - Think about what you would look for if you were sniffing traffic
- How likely do you suppose the existence of these servers would be?

DNS: History Lesson

- Domain Name Service provides a crucial mapping (RFC 1034)
  - Of what?
- Introduced in 1982, solved the problem of retrieving hosts.txt from an SRI computer
  - Why was this an issue?
  - How was this previous practice non-hierarchical?

DNS: Organization and Jargon

- DNS was designed to be highly hierarchical, i.e., in a tree structure
  - The root of the tree are the so-called root nameservers
  - How many are there?
  - Does this mean there are only that many physical servers?
  - Primarily situated in the U.S. (originally) and with its contents maintained by ICANN

DNS: Organization and Jargon

- Technically, a root name server:
  - Handles queries for the root **zone**
  - Returns a list of **authoritative** name servers for **top-level** domains
    - Currently 20 generic top-level domains and 248 country code top-level domains
- What is a zone?
- What is an authoritative name server?
- What is a top-level domain?

DNS: Jargon

- The concept of a zone is crucial for configuring the records for your DNS server
  - “A portion of the domain name space for which administrative responsibility has been delegated”
- Being authoritative is very important as well
  - Authoritative server provides actual answer to your DNS queries
  - Provides original and definitive answers to DNS queries
  - Master and slave set-up quite common

DNS: SOA

- Being authoritative for a zone requires creating an SOA on a DNS Server

```
name        ttl class rr    name-server email-addr  (sn ref ret ex min)
example.com.    IN    SOA   ns.example.com. hostmaster.example.com. (
                              2003080800 ; sn = serial number
                              172800     ; ref = refresh = 2d
                              900        ; ret = update retry = 15m
                              1209600    ; ex = expiry = 2w
                              3600       ; nx = nxdomain ttl = 1h
                              )
; the following are also valid using @ and blank
@               IN    SOA   ns.example.com. hostmaster.example.com. (
                IN    SOA   ns.example.com. hostmaster.example.com. (
```

DNS: SOA, Cont.

- SOA defines global parameters for the domain
- It’s the most complex and critical record in the zone file
  - Only one SOA per zone
  - Gets sent by the master to the slave
    - Updates get sent when the serial number changes
  - Always associated with an NS record

DNS: Record Types

- SOA is just one type of DNS record
- Many obscure DNS types exist, but there are a few standard ones that you must be familiar with
- A and AAAA records
  - These map what?
- PTR records
  - These make what type of query possible?

DNS: Record Types

- CNAME
  - Why is it useful to have canonical names?
- MX
  - Mail Exchanger
    - Also includes a preference value
  - Crucial for have a functioning SMTP server
- NS
  - Name server
  - Describes authoritative ones for the zone

DNS: Record Types

- SRV
  - Defines services available in the zone
  - E.g., LDAP, HTTP, XMPP
- TXT
  - Text information associated with a name
  - Associate arbitrary and unformatted text with a host or other name
  - Can add functionality through these records
    - Sender Policy Framework

DNS: Query Types

- Queries are central to DNS and are what its purpose is
- Several different ways that a query can be posed to a name server
- Will most queries to a DNS server be for domains for which it has local zone files?
  - What type of query is typically associated with not having a local zone file?

DNS: Recursive Query

- Where the DNS server will fully answer the query (or give an error)
  - NOT required to support recursive queries
  - Negotiate use of recursion using bits in the DNS query headers
- Three responses to a recursive query
  - Answer along w/ CNAME records
  - Error -> the domain or host non-existent
  - Temporary error indication

DNS: Recursion Example

- Query to local caching DNS for x.example.com
- Not found in cache
- Query to a root-server for IP of x.example.com
- Root replies with a referral to TLD for .com
- Local DNS query TLD server ✉ TLD’s referral
- Local DNS queries name server given
- Name server responds w/ CNAME and A
- Local DNS returns an answer

DNS: Other Query Types

- Iterative query (non-recursive)
  - Partial answer or error message
  - Must be supported by DNS servers
- Four possible iterative responses
  - Answer to the query along w/ CNAMEs
  - Error that host does not exist
  - Temporary error
  - A referral (may not be to an authoritative server)

DNS: Other Queries, Cont.

- Inverse queries
  - Historic anomaly not used too often
  - Completely optional
    - Rather than implementing, a server can return a **Not Implemented** response
  - Maps a resource record to a domain
    - Subtly different from a reverse mapping
    - What is the domain name for this MX record
  - Ended up not being used in practice (often the case with RFC features)

DNS: Types of Servers

- DNS servers often perform several different rules depending on the zone
  - But there are common types with specific names
- Master and slave arrangement (mentioned before)
  - Primarily for redundancy
  - Slave serves as a backup of the master
    - Slave gets it configuration from the master via zone xfer
    - The master gets it data from a local file system
  - These are approximately true but convey the sense of what these types of DNS servers entail

DNS: Types of Servers

- Caching name servers
  - Obtains mappings from other server
  - And then saves the data locally
    - Until the TTL value of the response expires
  - Non-authoritative responses come from a cache
- Forwarding name servers
  - Forwards all requests to another server
  - And caches the results

DNS: Types of Servers

- Stealth name server
  - Doesn’t appear in any publicly available NS record
- Authoritative only
  - Does not cache, i.e., no recursion
  - Only responds to requests for its delegated zone
- Split horizon
  - Gives different responses based on the source IP
  - Done for load balancing, naming consistency, and geographic mapping

DNS: Security

- Large and somewhat complicated issue
  - We will push it on the stack and pop it in a few weeks
- Many potential threats to the DNS system
  - One of the most common, and the one addressed by DNSSEC, relates to a lack of authentication
    - Same issue seen with DHCP
  - However, another major problem has to do with configuration errors ✉DNS Amplification attacks
    - What is an open resolver?

DNS: Packet Structure

- What all DNS has in common in a particular packet format

Domain Name System										
Bit Offset	0–15	16–31								
0	DNS ID Number	QR	OpCode	AA	TC	RD	RA	Z	RCode	
32	Question Count	Answer Count								
64	Name Server Count	Additional Records Count								
96	Questions Section	Answers Section								
128	Authority Section	Additional Information Section								

DNS: Simple Query

- Looking at the first packet trace, we can see the DNS query only requiring two packets
  - Query
    - Can tell based on the expanded flags section
    - Simple packet construction
  - Response
    - Quick and connectionless
    - But, uses an identification number to link this to the previous query

DNS: Recursive Packets

- Looks different from the client and server's perspective
  - Client simply requests recursion
    - If request is accepted, get a direct answer back
  - Server has to put in a lot more work
- If you were monitoring network activity, what related to DNS would you want to log?
  - Where should you place your network tap?
  - Is a full packet capture the best option here?

DNS: Zone Transfers

- Two types are available
  - AXFR (Full transfer)
  - IXFR (Incremental transfer)
- Typically done for redundancy purposes
  - Main difference in traffic is the transport protocol being used
  - Lots of data transferred with this request even for simple cases
  - Shows the disparity in response vs. query size that has plagued DNS based DoS attacks